OpenLLM

OpenLLM

Field	Value
Distribution	BSS — OpenSOF
Product	OpenSOF
Release	0.15.1
Deployment	`opensof.bss.dev`
Source	`/srv/bss/releases/OpenSOF-v0.15.0-20app`
Evidence	Catalog intent plus component-scoped static evidence
Source fingerprint	`cda583b42f2a0d296b268ab5b174932a378c8be6fb52ffa1af14af896e990f6e`
Status	Generated baseline — human review required

> **Verification boundary:** This page combines platform design guidance with static evidence from the release. It does not prove that every detected interface is enabled, reachable, secure, or operational in the deployed environment.

Purpose

The governed language-model interface for chat, retrieval, code pipelines and model selection across hosted and open-source models.

Operational value

Makes multiple models available through one operational entry point while letting workflows use the best model for the task.

Differentiators

LLMs can be constrained by platform semantics, source provenance and explicit pipelines instead of being asked to infer the entire mission context from prompts.

Platform connections

- OpenKnowledge
- OpenAnalytics
- OpenData
- OpenIIA

Release detection

Status	Score	Evidence items
detected	135	12

Evidence type	Source	Match
path	`lib/openllm.js`	`openllm`
path	`lib/openllm/agents.js`	`openllm`
path	`lib/openllm/pipeline-engine.js`	`openllm`
path	`lib/openllm/providers.js`	`openllm`
path	`lib/openllm/templates.js`	`openllm`
content	`server.js`	`openllm`
content	`lib/openllm.js`	`openllm`
content	`lib/openllm/agents.js`	`openllm`
content	`lib/openllm/pipeline-engine.js`	`openllm`
content	`lib/openllm/providers.js`	`openllm`
path	`public/open-llm/app.js`	`open-llm`
path	`public/open-llm/index.html`	`open-llm`

Candidate REST/API interfaces

No component-specific REST route was associated by the scanner.

Candidate real-time interfaces

No component-specific WebSocket endpoint was associated by the scanner.

Configuration candidates

Variable	Default	Evidence
`AEGIS_SENTINEL_LABEL`	COMPILED_DEPLOYMENT.aegisSentinelLabel).trim() || COMPILED_DEPLOYMENT.aegisSentinelLabel	server.js, tools/integrate_opensof_service_entries.py
`ANTHROPIC_API_KEY`	—	server.js, lib/openllm/agents.js, lib/openllm/providers.js
`API`	—	open-cybersec/app.js, public/open-cybersec/app.js, public/open-llm/app.js
`DATA_DIR`	path.join(ROOT	OPENCYBERSEC-QUICKSTART.md, OPENCYBERSEC.md, RELEASE-MANIFEST-v0.14.0.json, UPGRADE-v0.14.0.md
`EOD_TECH_TARGET`	@eodtech	server.js
`HOME`	/tmp	lib/openllm/pipeline-engine.js, openrf/agent/functions/start-5g-core.sh, openrf/agent/functions/status-5g-core.sh, third_party/ontowiki/.travis.yml
`HOST`	0.0.0.0	server.js, lib/openrf-controller/server.js
`KNOWLEDGE_NS`	—	server.js
`LANG`	C.UTF-8	lib/openllm/pipeline-engine.js
`MISSION_KNOWLEDGE_NS`	—	server.js
`MOUNT_PATH`	COMPILED_DEPLOYMENT.mountPath	server.js

Variable	Default	Evidence
`NODE_ID`	COMPILED_DEPLOYMENT.nodeId	server.js, edge/openssa-sensor/lib/openssa.js, lib/openssa.js
`OPENAAR_SIGNING_KEY`	[REDACTED]	server.js
`OPENAAR_SNAPSHOT_EVERY_EVENTS`	100	server.js
`OPENAAR_SNAPSHOT_INTERVAL_S`	30	server.js
`OPENAI_API_KEY`	—	server.js, lib/openllm/providers.js
`OPENANALYTICS_CONNECTOR_TIMEOUT_MS`	60000	server.js
`OPENBUS_API_TOKEN`	[REDACTED]	OPENKNOWLEDGE-OPENTASK.md, OPENLVC-DEMO.md, OPENLVC-RTI.md, demo_simulator.py
`OPENBUS_MAX_HISTORY`	500	server.js
`OPENCHAT_DEFAULT_TARGET`	#eod-ops	server.js
`OPENCOP_TRACK_URL`	https://opencop.c24.airoapp.ai/api/tracks	server.js
`OPENCOP_UI_URL`	BUILTIN_OPENCOP_UI_URL	server.js
`OPENCYBERSEC_AGENT_TOKEN`	[REDACTED]	OPENCYBERSEC-QUICKSTART.md, OPENCYBERSEC.md, server.js, examples/opencybersec/ingest-examples.sh
`OPENCYBERSEC_OPERATOR_TOKEN`	[REDACTED]	OPENCYBERSEC-QUICKSTART.md, OPENCYBERSEC.md, server.js, examples/opencybersec/ingest-examples.sh
`OPENCYBERSEC_READ_TOKEN`	—	server.js
`OPENFILES_HEALTH_URL`	—	server.js, tools/integrate_opensof_service_entries.py
`OPENFILES_SERVICE_URL`	—	server.js
`OPENIIA_MAX_EVIDENCE_BYTES`	12000000	server.js
`OPENISAC_HEALTH_URL`	—	server.js, tools/integrate_opensof_service_entries.py
`OPENISAC_SERVICE_URL`	—	server.js
`OPENKNOWLEDGE_EDITOR_TOKEN`	[REDACTED]	server.js
`OPENKNOWLEDGE_GRAPH`	https://opensof.local/graph/core	server.js
`OPENKNOWLEDGE_MODEL_FILE`	path.join(DATA	server.js
`OPENKNOWLEDGE_ONTOWIKI_URL`	—	server.js

Variable	Default	Evidence
`OPENKNOWLEDGE_SPARQL_ENDPOINT`	—	server.js
`OPENKNOWLEDGE_TIMEOUT_MS`	8000	server.js
`OPENLLM_AGENT_MAX_OUTPUT_BYTES`	—	lib/openllm/agents.js
`OPENLLM_AGENT_TIMEOUT_MS`	—	lib/openllm/agents.js
`OPENLLM_ALLOW_LOCAL_EXECUTION`	—	lib/openllm/pipeline-engine.js
`OPENLLM_ANTHROPIC_API_KEY`	[REDACTED]	server.js, lib/openllm/providers.js
`OPENLLM_ANTHROPIC_URL`	https://api.anthropic.com/v1').replace(//+$/	lib/openllm/providers.js
`OPENLLM_ANTHROPIC_VERSION`	2023-06-01	lib/openllm/providers.js
`OPENLLM_CLAUDE_BIN`	claude	lib/openllm/agents.js
`OPENLLM_CODEX_BIN`	codex	lib/openllm/agents.js
`OPENLLM_COMMAND_MODE`	off').toLowerCase(	lib/openllm/pipeline-engine.js
`OPENLLM_FALLBACK_WRITE_MAX_BYTES`	—	lib/openllm/pipeline-engine.js
`OPENLLM_HEALTH_TIMEOUT_MS`	—	lib/openllm/providers.js
`OPENLLM_MAX_AUDIT`	—	lib/openllm.js
`OPENLLM_MAX_RUNS`	—	lib/openllm/pipeline-engine.js
`OPENLLM_MODEL_CACHE_TTL_MS`	—	lib/openllm/providers.js
`OPENLLM_OPENAI_API_KEY`	[REDACTED]	server.js, lib/openllm/providers.js
`OPENLLM_OPENAI_URL`	https://api.openai.com/v1').replace(//+$/	lib/openllm/providers.js
`OPENLLM_OPENBUS_SCHEMA`	opensof.openbus.event/1.0	lib/openllm.js
`OPENLLM_OPENWEBUI_API_KEY`	[REDACTED]	server.js, lib/openllm/providers.js
`OPENLLM_OPENWEBUI_CHAT_PATH`	/api/chat/completions	lib/openllm/providers.js
`OPENLLM_OPENWEBUI_HEALTH_PATH`	/health	lib/openllm/providers.js
`OPENLLM_OPENWEBUI_MODELS_PATH`	/api/models	lib/openllm/providers.js
`OPENLLM_OPENWEBUI_URL`	process.env.OPENWEBUI_URL ||	server.js, lib/openllm/providers.js
`OPENLLM_OPERATOR_TOKEN`	[REDACTED]	server.js, lib/openllm.js
`OPENLLM_PROVIDER_TIMEOUT_MS`	—	lib/openllm/providers.js
`OPENLLM_QWEN_BIN`	qwen	lib/openllm/agents.js
`OPENLLM_SANDBOX_CPUS`	2	lib/openllm/pipeline-engine.js
`OPENLLM_SANDBOX_IMAGE`	openc5isr-openllm-sandbox:0.1.0	lib/openllm/pipeline-engine.js
`OPENLLM_SANDBOX_MEMORY`	2g	lib/openllm/pipeline-engine.js

Variable	Default	Evidence
`OPENLLM_SANDBOX_PIDS`	256	lib/openllm/pipeline-engine.js
`OPENLLM_WORKSPACES_DIR`	path.join(ROOT	server.js
`OPENLVC_HEALTH_URL`	—	server.js, tools/integrate_opensof_service_entries.py
`OPENLVC_SERVICE_URL`	—	server.js
`OPENMAIL_HEALTH_URL`	—	server.js, tools/integrate_opensof_service_entries.py
`OPENMAIL_SERVICE_URL`	—	server.js
`OPENRF_AGENT_TOKEN`	[REDACTED]	server.js, lib/openrf-controller/server.js, openrf/API.md
`OPENRF_DATA_DIR`	path.join(DATA	server.js, lib/openrf-controller/server.js
`OPENRF_OPERATOR_TOKEN`	[REDACTED]	server.js, lib/openrf-controller/server.js, openrf/API.md, openrf/README-UPSTREAM-v0.3.0.md
`OPENRF_READ_TOKEN`	—	server.js, lib/openrf-controller/server.js, openrf/API.md
`OPENSSA_ACTIVE_TIMEOUT_S`	900	server.js, edge/openssa-sensor/SERVER_INTEGRATION.md, edge/openssa-sensor/lib/openssa.js, lib/openssa.js
`OPENSSA_ITU_REGION`	2	server.js, edge/openssa-sensor/SERVER_INTEGRATION.md, edge/openssa-sensor/lib/openssa.js, lib/openssa.js
`OPENSSA_SENSOR_TOKEN`	[REDACTED]	server.js, edge/openssa-sensor/SERVER_INTEGRATION.md, edge/openssa-sensor/local_server.js, edge/openssa-sensor/demo/run_streaming_demo.py
`OPENWEBUI_API_KEY`	[REDACTED]	server.js, lib/openllm/providers.js
`OPENWEBUI_CHAT_PATH`	/api/chat/completions	server.js
`OPENWEBUI_DEFAULT_MODEL`	—	server.js

Service candidates

No component-specific service definition was associated by the scanner.

External dependencies/endpoints

Host	URL	Source
${req.headers.host	`http://${req.headers.host/`	`server.js`
177.75.6.125	`http://177.75.6.125:3000/`	`lib/openllm/providers.js`
api.anthropic.com	`https://api.anthropic.com/v1`	`lib/openllm/providers.js`
api.openai.com	`https://api.openai.com/v1`	`lib/openllm/providers.js`
opencop.c24.airoapp.ai	`https://opencop.c24.airoapp.ai/api/tracks`	`server.js`
opensof.bss.dev	`https://opensof.bss.dev/`	`server.js`
opensof.local	`https://opensof.local/graph/core`	`server.js`
opensof.local	`https://opensof.local/ontology`	`server.js`
opensof.local	`https://opensof.local/resource/`	`server.js`

Verification checklist

- Confirm the component is included and enabled in this edition/release.
- Record its authoritative service, process/container, port, base URL and health endpoint.
- Exercise its primary operator workflow and capture expected versus actual results.
- Verify authentication, authorization, audit, error behavior and data handling policy.
- Verify OpenBus/OpenKnowledge relationships and time/provenance metadata where applicable.
- Document known limitations and the release in which they are corrected.

Maintainer Notes

Add human-reviewed deployment notes, corrections, decisions, screenshots, and links here. Content outside the generated block is preserved on future runs.

Revision #1
Created 2026-08-28 15:10:49 UTC by Nexus Ops Administrator
Updated 2026-08-28 15:10:49 UTC by Nexus Ops Administrator